UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The person of CHAD BAUER, DOB 05/XX/1999, SSN XXX-XX-1729

Case No. **1:22-MJ-00539**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A (incorporated by reference).

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B (incorporated by reference).

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 922(a)(6), 1341, 1343, 1349, 1028A, 371	False Statement During Purchase of a Firearm, Mail Fraud, Wire Fraud, Conspiracy to Commit Mail and Wire Fraud, Aggravated Identity Theft, Conspiracy to Commit an Offense Against the United States

The application is based on these facts:

See Attached Affidavit (incorporated by reference).

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Derek Graham
Applicant's signature

Derek Graham, Special Agent, ATF
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by FaceTime Video Conference *(specify reliable electronic means)*.

Date: **Sep 14, 2022**

Stephanie K. Bowman
Judge's signature

City and state: Cincinnati, Ohio

Hon. Stephanie K. Bowman, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Person to be Searched

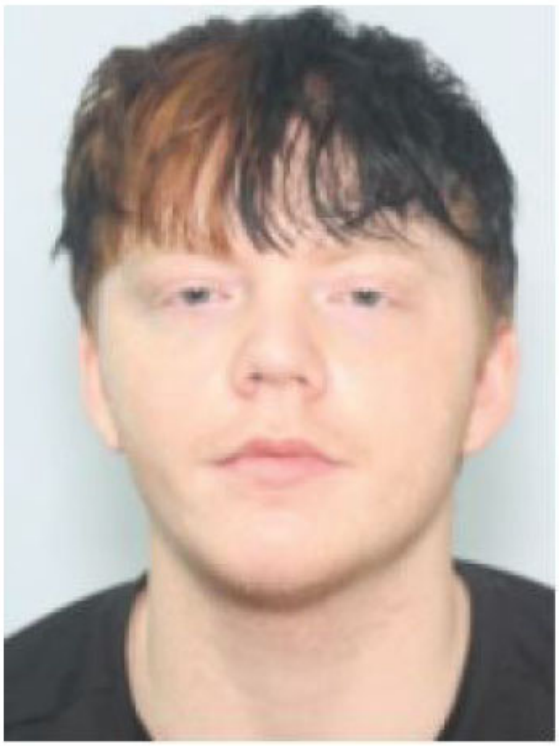
CHAD BAUER

White Male, 6'01", 225 lbs

DOB 05/XX/1999

SSN XXX-XX-1729

This warrant authorizes a search of the person of CHAD BAUER, including all pockets, containers, backpacks, bags, purses, or other containers on his person or within his immediate reach at the time of the search.



ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 922(a)(6) (False Statement During Purchase of a Firearm), 1341 (Mail Fraud), 1343 (Wire Fraud), 1349 (Conspiracy to Commit Mail and Wire Fraud), 1028A (Aggravated Identity Theft), and 371 (Conspiracy to Commit an Offense Against the United States) (collectively, the "Target Offenses"), those violations involving NEHEMIAH JONES, ZEPHANIAH JONES, CHAD BAUER, and other known and unknown coconspirators and occurring after on or about April 8, 2022, including:

   a. Records and information relating to the purchase, attempted purchase, acquisition, possession, sale, and/or transfer of firearms, ammunition, and/or firearms accessories;
   b. Records and information relating to the possession, theft, use, and/or transfer of personally identifiable information and financial information, including but not limited to credit card information;
   c. Records and information relating to the identity of coconspirators to the scheme under investigation;
   d. Records and information relating to preparatory steps taken in furtherance of the scheme to defraud;
   e. Records and information relating to steps taken to evade capture for the Target Offenses;
   f. Records and information relating to communications between any coconspirators involved in the Target Offenses;

g. Records and information relating to the proceeds of the scheme, including but not limited to information about financial accounts used to receive, possess, store, and transfer criminal proceeds;

h. Records and information relating to who has occupancy and control over the premises searched, including but not limited to keys, rental agreements and records, leases, mail, vehicle registrations, utility bills and receipts, and personal identification and photographs.

2. Firearms, ammunition, holsters, gun cases, gun boxes, and other firearms accessories.

3. Purchase and sale documents and receipts relating to firearms, ammunition, and firearms accessories.

4. Any U.S. currency in an amount of at least $100 that constitutes evidence of, or the proceeds of, illegal firearm sales.

5. Financial instruments used in furtherance of violations of the Target Offenses, or that constitute proceeds of violations of the Target Offenses, including but not limited to credit cards, debit cards, prepaid cards, money orders, and cashier's checks.

6. Computers or storage media used as a means to commit the violations described above.

7. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs,

registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF THE PERSON OF CHAD BAUER, DOB 05/XX/1999, SSN XXX-XX-1729	Case No. **1:22-MJ-00539** **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Derek Graham, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Federal Rule of Criminal Procedure 41 for a warrant to search the person of **CHAD BAUER, DOB 05/XX/1999, SSN XXX-XX-1729** (the **"SUBJECT PREMISES"**), further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF), and have been so employed since October of 2007. As a part of my training with the ATF, I graduated from the Federal Law Enforcement Training Center, Criminal Investigator School, located in Brunswick, Georgia. I graduated from the ATF Special Agent Basic Training Academy, located in Brunswick, Georgia, in April 2008. Prior to my employment with ATF, I was a Federal Air Marshal in the Department of Homeland Security from June 2006 through October 2007. In addition, I was a Criminal Research Specialist with the Washington, DC High Intensity Drug Trafficking Area/Drug Enforcement Administration from June 2003 through June 2006. I am a graduate of Augustana College, where I received a Bachelor's degree in Business Administration in May of 2002. I am also a graduate of Boston University, where I received a master's degree in Criminal Justice in June of 2006.

3. I have experience in the investigation, apprehension, and prosecution of individuals suspected of being involved in federal firearms and drug offenses. I have specific experience in investigating the use of cell phones by criminal suspects who are involved in the commission of those offenses. I have been trained by ATF as a Digital Media Collection Specialist (DMCS) and have completed more than 285 forensic extractions of cellular telephones, computers, and other electronic storage media. I have also reviewed forensic extractions of cellular telephones, computers, and other electronic storage media, and have examined content and communications contained within these devices obtained by forensic extraction. This content includes records of communication through call logs, text message content, images and videos, and communication made through various social media applications.

4. I know from training and experience that individuals typically keep cell phones on their persons or within their immediate control, such as in the cupholder of a car they are driving, because cell phones are regularly used and possessed as an item of personal property. I also know from my training and experience that in today's age it is typical for individuals engaged in criminal activity to possess multiple active cellular phones at one time. For example, many criminals have one phone that they use for personal communications (e.g., with family members) and another phone that they use to communicate with criminal associates.

5. I also know from I also know based on my training and experience that, when individuals are involved in an illegal business, such as firearms or drug trafficking, those individuals commonly maintain on their electronic devices lists of customers, supplier lists, pay/owe sheets, receipts, address books, and other documents listing the price and quantity of items sold, as well as the date the items were purchased, possessed, and sold.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 922(a)(6) (False Statement During Purchase of a Firearm), 1341 (Mail Fraud), 1343 (Wire Fraud), 1349 (Conspiracy to Commit Mail and Wire Fraud), 1028A (Aggravated Identity Theft), and 371 (Conspiracy to Commit an Offense Against the United States) (collectively, the "Target Offenses") have been committed by ZEPHANIAH JONES, NEHEMIAH JONES, CHAD BAUER, and other known and unknown coconspirators. There is also probable cause to search the premises described in Attachment A for the evidence, instrumentalities, fruits, and contraband of these crimes further described in Attachment B.

PROBABLE CAUSE

A. ATF and the U.S. Attorney's Office are investigating a fraud scheme in which the perpetrators use stolen credit card information to purchase firearms online and have them shipped to Cincinnati.

9. From on or about April 8, 2022, through on or about June 22, 2022, certain individuals made more than 376 attempts to purchase firearms online and/or to have them transferred by mail to various Federal Firearms Licensees (FFLs) in the Southern District of Ohio, where the transactions could be completed and the firearms could be picked up. Some of these orders were placed in the name of ZEPHANIAH JONES, NEHEMIAH JONES, and CHAD BAUER, among others. Many, and possibly all, of the purchases and attempted purchases were made using stolen credit card information.

10. Many of the attempted purchases were not successfully processed, apparently either because there was a problem with the stolen credit card information or because the gun

dealer's fraud-detection system prevented the transaction from occurring. But further investigation has shown that, after some purchases went through, and the firearms were shipped to Cincinnati, some of the suspects named above arrived at FFLs in this District and completed, or attempted to complete, the transfers.[1] During some of those in-person interactions, the suspects have represented that they were the true purchasers of the firearms but have made statements or taken other actions suggesting that, in fact, they were buying the firearms for someone else. Some of the suspects have also provided false information about their residences on ATF Form 4473 – Firearms Transaction Record ("ATF Form 4473"). Several of these in-person transfers at local FFLs were identified as straw purchases and were denied; however, at this stage of the investigation, I have identified approximately 50 firearms that were transferred to the suspects.

11. I am now seeking a warrant authorizing the search of the person of CHAD BAUER. As described in more detail below, there is probable cause to believe that a search of BAUER's person will reveal the items described in Attachment B, which are evidence, instrumentalities, fruits, and contraband of violations of the Target Offenses. These items include but are not limited to electronic devices used in furtherance of, or that contain evidence of, the Target Offenses; firearms, ammunition, and firearm paraphernalia; records related to firearms

[1] Based on my training and experience, I know that a sale of a firearm through an FFL is required to take place in the same State as which the individual is a resident. If an individual purchases a firearm from an FFL from another State, the FFL will transfer the firearm to an FFL within the individual's State of residence. The FFL in the receiving State may then complete the transfer, and finalize the sale, by having the purchasing individual complete an ATF Form 4473. An FFL participating in the final stage of the transfer to the purchasing individual generally charges a nominal fee for the service.

and firearms purchases or transfers; and evidence relating to the possession and use of stolen credit card information.

B. IP information links hundreds of the attempted fraudulent purchases to NEHEMIAH and ZEPHANIAH JONES, who have completed some of the transfers in person.

12. Records from Guns.com show that hundreds of the fraudulent attempted orders of firearms, in many different names, were placed from IP address 52.124.36.227 ("IP 227"). Records from the internet service provider show that IP 227 services the apartment complex at 424 Straight Street in Cincinnati, where NEHEMIAH JONES and ZEPHANIAH JONES were tenants as of July 2022. Relevant details of some of those orders are as follows:

Name	Date(s)	Attempts	Email(s)	Billing Address(es)
ANEESAH WILLIAMS	4/28 – 6/4/22	67	CLEARY091150 @GMAIL.COM ANEESAHWILLIAMS10 @GMAIL.COM ANEESAHW1994 @GMAIL.COM	• [Redacted] Princeton Glendale Road, Cincinnati, OH 45246 • [Redacted] Curry Drive Cleveland OH 44124 • [Redacted] Kellie Lane Sylvania OH 43560 • [Redacted] Twin Spires Dr Batavia OH 45103 • [Redacted] state route 39 Walnut Creek OH, 44687; • [Redacted] Kalklosch Road Logan OH, 43138 • [Redacted] Orders Road Grove City OH, 43123 • [Redacted] East High Street Mantua OH, 44255 • [Redacted] Smiley Ave Westlake OH, 44145 • [Redacted] Gatehouse Lane Columbus OH, 43235 • [Redacted] West Exchange Street Akron OH, 44313 • [Redacted] Saint Andrews Drive Westerville OH, 43082 • [Redacted] Maplebrooke Drive East Westerville OH, 43082 • [Redacted] West Law Road Valley City OH, 44280

				• [Redacted] Weston Park Drive Powell OH, 43065
MYKIA MELTON	5/25 – 5/26/22	37	RAYNELLPARKS @GMAIL.COM	• [Redacted] Smiley Ave West lake OH, 44145 • [Redacted] Gatehouse Lane Columbus OH, 43235 • [Redacted] West Exchange Street Akron OH, 44313 • [Redacted] Saint Andrews Drive Westerville OH, 43082 • [Redacted] Maplebrooke Drive East Westerville OH, 43082 • [Redacted] East High Street Mantua OH, 44255
KIANA HARRELL	5/27-5/28/22	39	RAYNELLJONES80 @GMAIL.COM	• [Redacted] Greenoak Dr Cincinnati OH, 45248 • [Redacted] Warrensburg Road Delaware OH, 43015 • [Redacted] Kennard Road Medina OH, 44256 • [Redacted] Crary Lane Willoughby OH, 44094 • [Redacted] E Lincoln Highway Lima OH, 45807 • [Redacted] Wickliffe Road Columbus OH, 43221 • [Redacted] Niderdale Way Middletown OH, 45042
NEHEMIAH JONES	5/30-6/3/22	22	NEHEMIAHJ470 @GMAIL.COM	• [Redacted] Niderdale Way Middletown OH, 45042 • [Redacted] Windward Circle Aurora OH, 44202 • [Redacted] Lightwind Court Westerville OH, 43081 • [Redacted] Woodstock Drive Avon Lake OH, 44012 • [Redacted] Franks Road Southeast Heath OH, 43056 • [Redacted] Beachview Road Willoughby OH, 44094 • [Redacted] Kinsman Court Columbus OH, 43207
NEHEMIAH JONES	4/8-4/23/22	7	SPEEDKILLER2108 @GMAIL.COM	• [Redacted] Parkside Drive Parma OH, 44130 • [Redacted] Morse rd columbus OH, 43230 • [Redacted] Glenwood Dr Twinsburg OH, 44087

				• [Redacted] Glen Allen Drive Cleveland Heights OH, 44121
JERIN JOHNSON SR.	6/20-6/22/22	47	OFFICIALK2163@GMAIL.COM	• [Redacted] Public Square Cleveland OH, 44113 • [Redacted] Mc Intosh Road Pataskala OH, 43062 • [Redacted] Public Square Cleveland OH, 44113 • [Redacted] Township Road 162 Cardington OH, 43315 • [Redacted] 2nd Street Clarksville OH, 45113 • [Redacted] Holloway Rd Holland OH, 43528
Kashawna Fisher	4/22 – 4/28/22	26	DJOMKAMALVINEE@GMAIL.COM	• [Redacted] Northfield Court Springfield OH, 45502 • [Redacted] Southwood Drive Lima OH, 45805 • [Redacted] Northfield Court Springfield OH, 45502 • [Redacted] Croydon Drive Northwest Canton OH, 44718 • [Redacted] Northfield Court Springfield OH, 45502 • [Redacted] Tanbark Lane Strongsville OH, 44149
ZEPHANIAH JONES[2]	4/10-4/22/22	6	ZEPH21J@ICLOUD.COM	• [Redacted] Shepherds Way Batavia OH, 45103 • O'Bryan Place Centerville OH, 45459 • [Redacted] Dover Center Road Bay Village OH, 44140 • [Redacted] Walden Glen Circle Cincinnati OH, 45231 • [Redacted] Dill Road Cleveland OH, 44121
Dewayna Stevens	4/11/22	4	MARYVENO1937@GMAIL.COM	• [Redacted] Tara Boulevard Jonesboro GA, 30236 • [Redacted] Ellis Street Metter GA, 30439 • [Redacted] Newcastle Circle Stonecrest GA, 30038

[2] A query in OHLEG, a database available to law enforcement, showed that NEHEMIAH JONES and ZEPHANIAH JONES were issued Ohio Identification Cards with the same home address on them. This leads me to believe that the two are relatives, possibly brothers.

13. Both ZEPHANIAH JONES and NEHEMIAH JONES have arrived at Cincinnati-area FFLs to complete some of these firearms transfers of firearms purchased with suspected stolen credit card information. Specifically, NEHEMIAH JONES completed at least two transfers, and ZEPHANIAH JONES completed transfers of at least seven firearms between April 1 and July 12, 2022.

C. The phone number used for 11 attempted purchases under WILLIAMS's name was also used for suspected fraudulent orders placed in CHAD BAUER's name; BAUER completed some of these transfers.

14. Eleven attempted orders in ANEESAH WILLIAMS's name were placed with Guns.com on April 28, 2022. The phone number associated with these orders was 330-XXX-0471 (the "0471 Number").

15. Records from a Tennessee FFL, Smoky Mountain Guns, show that the 0471 Number was also listed as the buyer's phone number a few days earlier, on April 23, 2022, for two online orders of firearms under the name CHAD BAUER. The first was an order for two FN-manufactured pistols and one Glock pistol, and the second order was for a Glock pistol. The billing address on both orders was an address on Sugar Loaf Lane in Murrells Inlet, SC.

16. The firearms were shipped to North College Hill Store, where BAUER picked them up on April 30, 2022. On the ATF Form 4473, BAUER listed his home address not as the South Carolina address on the order, but as an address on Carter Ave. in Cincinnati, Ohio, as confirmed by his driver's license. For both of the orders under BAUER's name, the associated email address was MARYVENO1937@GMAIL.COM, which records from Google show was logged into from IP 227, linked to ZEPHANIAH JONES and NEHEMIAH JONES, as described above. BAUER also represented on the Form 4473 that he was the true purchaser of the firearms.

D. After BAUER picked up a firearm that had been ordered in his name from FFL Suppressive Fire, the credit card company initiated a chargeback, and a suspect taunted the FFL via text about the loss.

17. On or about May 6, 2022, at Target World in Cincinnati, CHAD BAUER completed the transfer of an FN Five-Seven MK2P pistol that had been ordered in his name from FFL Suppressive Fire in Florida. The IP address associated with the order was IP 227, linked to ZEPHANIAH and NEHEMIAH JONES, as described above. The phone number on the order was the 0471 Number, which, as described above, was also used on other orders placed under the names of ANEESAH WILLIAMS and CHAD BAUER. On the Form 4473, BAUER once again represented that he was the true purchaser of the firearm.

18. After the transfer was completed, the credit card company initiated a chargeback based on suspected fraud. A representative from Suppressive Fire then sent text messages to the 0471 Number asking for the firearm to be returned. During that conversation, the user of the phone taunted the employee, saying that the paperwork had already been completed and that the firearm would not be registered to his (the person using the 0471 Number's) name. An excerpt of this text transaction follows:

FFL employee	calling you from suppressive fire. You charged back your credit card for the gun you purchased from us
0471 Number	I don't recall
FFL employee	You bought a gun from us, then you called your credit card company to reverse the charge
0471 Number	What type of gun
FFL employee	The FN 5.7 you bought from us
0471 Number	Oh okay have a nice day
FFL employee	This is how this works, this gun is now considered stolen, you've got 24 hours to contact the bank, get the money put back in our account or we contact the ATF and the Ohio state police

0471 Number	Check the Ohio laws guns don't register to your name when you buy them [heart-hands emoji] Paper work already done
FFL employee	Form 4473, that you filled out for your background check, the gun and your info are on it. I'll send the stolen gun report tonight, you made a poor decision We will file a lawsuit in Florida as well, I've got a guy who does this for all the dealers, bad plan fella
0471 Number	Nice

19. Based on my training and experience and knowledge of this investigation, as well as because the user of the 0471 Number seemed unconcerned about being linked to the stolen firearm, I believe the 0471 Number is likely not used by CHAD BAUER—whose name was indeed on the Form 4473 linked to the transfer—but by the person who placed the online order. I further believe that the person who placed the online was order was likely ZEPHANIAH JONES or NEHEMIAH JONES, given that it was placed from IP 227, linked to their address. Based on my training and experience and knowledge of this investigation, I believe ZEPHANIAH JONES and NEHEMIAH JONES have placed many online orders for firearms using fraudulent credit card information and have enlisted other individuals, such as CHAD BAUER, to illegally complete the transfers in a so-called "straw purchase" and then give the firearms to ZEPHANIAH JONES and/or NEHEMIAH JONES.

E. A review of other coconspirators' cellular telephones seized in July 2022 revealed communications related to firearms transfers.

20. From on or about July 28, 2022, through present, I have reviewed multiple extractions of cellular telephones possessed by other suspects identified in this investigation. I identified multiple conversations related to the transfer of firearms on behalf of other individuals consistent with the information known in this investigation. For example, a phone used by

JERIN JOHNSON, SR.—one of the individuals in whose name online orders were placed from IP 227—contained text messages between him and ZEPHANIAH JONES showing that ZEPHANIAH JONES was buying firearms, sharing tracking information (such as from UPS) showing when the firearms were delivered to local FFLs, and directing JOHNSON to pick the firearms up.

21. Based on this information and other evidence described in this affidavit, I submit that there is probable cause to believe that the perpetrators of the scheme described in this affidavit used cellular telephones to communicate about the scheme and to receive notifications relating to the firearms purchases and deliveries. Additionally, based on my training and experience investigating straw-purchasing schemes, as well as the information I describe below about records likely to be stored on cellular phones, I further submit that there is probable cause to believe that any cellphones associated with CHAD BAUER will contain location information, search queries, images and videos, receipts, stored emails, financial records, and other records that are evidence of violations of the Target Offenses.

F. A representative of Guns.com confirmed that shipping updates are sent to purchasers via email and that the firearms are shipped to local FFLs via UPS.

22. In June 2022, I spoke with a representative of Guns.com with knowledge of the Guns.com order process. That representative explained that, when an order is placed via Guns.com, a confirmation email is sent to the email account associated with the order. Shipping updates are also sent to the customer via email. The representative explained that these shipping updates are not sent via text message.

23. The representative of Guns.com also confirmed that, when an online order is placed for a transfer to a local FFL, the firearm is shipped via the interstate carrier UPS.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

24. As described above and in Attachment B, this application seeks permission to search for, among other things, records that might be found on the person of CHAD BAUER (i.e., the **SUBJECT PREMISES)**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

25. *Probable cause.* I submit that if a computer or storage medium is found on the **SUBJECT PREMISES**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

A. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

B. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

C. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

D. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **SUBJECT PREMISES** because:

A. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

B. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that

log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

C. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

D. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

E. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

27. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either

seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

A. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

B. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

C. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

29. I submit that this affidavit supports probable cause for a warrant to search the person of CHAD BAUER, further described in Attachment A, and seize the items described in Attachment B.

//

//

//

//

//

//

//

//

//

REQUEST FOR SEALING

30. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Derek Graham

DEREK GRAHAM
Special Agent
Bureau of Alcohol, Tobacco, Firearms and Explosives

Subscribed and sworn to before me via FaceTime videoconference on September 14, 2022.

Stephanie K. Bowman

HON. STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Person to be Searched

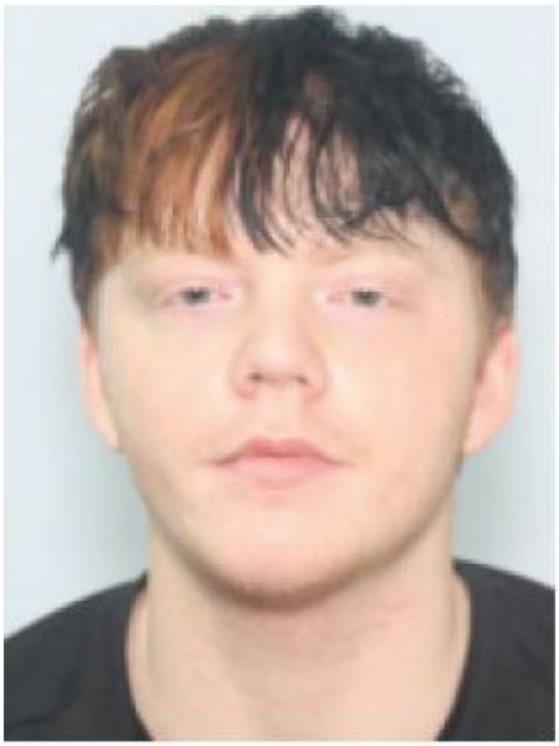
CHAD BAUER

White Male, 6'01", 225 lbs

DOB 05/XX/1999

SSN XXX-XX-1729

This warrant authorizes a search of the person of CHAD BAUER, including all pockets, containers, backpacks, bags, purses, or other containers on his person or within his immediate reach at the time of the search.



ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 922(a)(6) (False Statement During Purchase of a Firearm), 1341 (Mail Fraud), 1343 (Wire Fraud), 1349 (Conspiracy to Commit Mail and Wire Fraud), 1028A (Aggravated Identity Theft), and 371 (Conspiracy to Commit an Offense Against the United States) (collectively, the "Target Offenses"), those violations involving NEHEMIAH JONES, ZEPHANIAH JONES, CHAD BAUER, and other known and unknown coconspirators and occurring after on or about April 8, 2022, including:

   a. Records and information relating to the purchase, attempted purchase, acquisition, possession, sale, and/or transfer of firearms, ammunition, and/or firearms accessories;
   b. Records and information relating to the possession, theft, use, and/or transfer of personally identifiable information and financial information, including but not limited to credit card information;
   c. Records and information relating to the identity of coconspirators to the scheme under investigation;
   d. Records and information relating to preparatory steps taken in furtherance of the scheme to defraud;
   e. Records and information relating to steps taken to evade capture for the Target Offenses;
   f. Records and information relating to communications between any coconspirators involved in the Target Offenses;

g. Records and information relating to the proceeds of the scheme, including but not limited to information about financial accounts used to receive, possess, store, and transfer criminal proceeds;

h. Records and information relating to who has occupancy and control over the premises searched, including but not limited to keys, rental agreements and records, leases, mail, vehicle registrations, utility bills and receipts, and personal identification and photographs.

2. Firearms, ammunition, holsters, gun cases, gun boxes, and other firearms accessories.

3. Purchase and sale documents and receipts relating to firearms, ammunition, and firearms accessories.

4. Any U.S. currency in an amount of at least $100 that constitutes evidence of, or the proceeds of, illegal firearm sales.

5. Financial instruments used in furtherance of violations of the Target Offenses, or that constitute proceeds of violations of the Target Offenses, including but not limited to credit cards, debit cards, prepaid cards, money orders, and cashier's checks.

6. Computers or storage media used as a means to commit the violations described above.

7. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs,

registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.